PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number
20423-07775

Pursuant to 240 OG 45 and the *Legal Framework For EFS-Web*, I hereby certify that this follow-on correspondence is being officially submitted through the USPTO EFS-Web system from the Pacific Time Zone of the United States on the local date shown below.

on June 15, 2007

Signature /Brian Hoffman/

Typed or printed name Brian M. Hoffman

Application Number 10/612,198	Filed July 1, 2003
First Named Inventor Carey S. Nachenberg	
Art Unit 2137	Examiner Jaric E. Loving

This request is being filed with a notice of appeal.

I am the

□ applicant/inventor.

□ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.

☒ attorney or agent of record.
Registration number 39,713.

□ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 ______________

/Brian Hoffman/
Signature

Brian M. Hoffman
Typed or printed name

(415) 875-2484
Telephone number

June 15, 2007
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 1 of 1 forms is submitted.

ATTACHMENT TO THE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Pre-appeal review is requested because the rejections of record are clearly improper and without and factual or legal basis. Applicant respectfully requests that the panel reconsider and lift the rejections of record.

I. Status of Application

Examiner Loving issued a first Office Action in this application on July 7, 2006 rejecting all pending claims. Applicants submitted an Amendment in response on October 19. Examiner Loving issued a second Office Action on January 17, 2007 making a final rejection based on the same grounds as the first Office Action.

Applicants' representative conducted an interview with Examiner Loving on April 23, 2007 which focused on claims 20 and 21. Applicants' representative argued that the cited references did not show elements of these claims. Examiner Loving agreed to consult with a primary examiner regarding these arguments. This agreement is described by the Interview Summary in the record and identified as Paper No. 20070424.

On April 26, 2007, Applicants' representative called Examiner Loving to inquire as to the results of the consultation. Examiner Loving replied that he had spoken with a primary examiner and agreed that he would conduct a new search and issue a new office action if warranted. This agreement is described by the Interview Summary in the record and identified as Paper No. 20070426.

The application was subsequently transferred to Examiner Davis. Applicants' representative and Examiner Davis discussed the status of the application in early June 2007. Examiner Davis agreed to consider to consider Applicants arguments regarding the references, but did not agree to conduct a new search or issue a new office action at that time. Since the rejections on the record are clearly improper, Applicants hereby submit this Request for Review and request that a new search be conducted, and a new Office Action or Notice of Allowance be issued, for the reasons presented in the April 23 interview and described below.

II. Status of Claims

Claims 1 and 3-21 are pending and stand rejected. The claims relate to a database intrusion detection system. Generally, the claimed invention observes commands that are accessing a database and derives, from those commands, a set of acceptable commands. Claim 20 recites the observing and deriving elements, and further recites comparing commands received during an operational phase with the set of acceptable commands. Claim 21 explicitly recites that commands are observed during a training phase and compared during an operational phase.

Independent claims 1, 16, and 20, as originally filed, used the phrase "a computer code intrusion detection system." Claim 2 recited "wherein the computer code is a database, and the computer code intrusion detection system is a database intrusion detection system." In the October 19, 2006 Amendment, Applicants canceled claim 2 and amended the remaining claims to use the word "database" in place of "computer code." No other substantive amendments were made.[1]

[1] Because the amendment merely canceled a dependent claim and added its limitations into an independent claim, a subsequent office action based on new grounds of rejection should be non-final because the new rejection is not necessitated by Applicants' amendment. MPEP 706.07(a).

III. **Claim Rejection: Claim 20**

Claim 20 was rejected under § 103(a) as being unpatentable over U.S. Pat. Pub. No. 2003/0188189 to Desai et al. ("Desai") in view of U.S. Patent 6,775,827 to Harkins. This rejection is clearly in error because the proposed combination does not disclose the limitations:

> a training module adapted for observing, in real time, commands that are accessing the database, and for deriving from said commands, in real time, a set of acceptable commands; and
> coupled to the set of acceptable commands, a comparison module for comparing commands that access the database during an operational phase with commands in the set of acceptable commands.

In the final Office Action, the examiner stated that Desai discloses a database intrusion detection system and cites to paragraphs [0035], [0043], [0052], and [0056]. However, Desai in fact discloses a general intrusion detection and response system that analyzes data to identify normal and abnormal data traffic patterns. Desai never specifically discusses database intrusion attacks. Paragraphs [0035] and [0043] describe how Desai can observe traffic in real time and paragraph [0052] describes using an attack signature database. Paragraph [0056] mentions monitoring SQL traffic for abnormal behavior, but provides no teaching or suggestion of how to detect database intrusions based on this monitoring.

In fact, the Examiner acknowledges that Desai fails to disclose both the training and comparison modules and relies on Harkins for showing these elements. Harkins, however, is clearly off point. Harkins discloses an automated method for generating an audit record of a computer program for debugging purposes. At col., 4, lines 13-17, Harkins describes a method for providing real-time analysis of an executing program but does not teach or suggest that the executing program is accessing a database. Therefore, Harkins does not teach or suggest "observing…commands that are accessing [a] database" as claimed.

The Examiner asserts that Harkins teaches the training module at col. 5, lines 41-49. This portion merely discloses that Harkins uses default initial execution profiles that describe the execution options for the program being debugged. The Examiner asserts that the execution profiles contain frequently selected commands and are thus similar to a set of acceptable commands. However, the execution profiles are utilized to detect faults in programs; the fact that an execution profile is frequently selected does not imply that any commands in the profile are acceptable. Rather, the commands are merely used to understand the operation of the program being debugged.

The Examiner asserts that "comparing commands that access the database during an operation phase with commands in the set of acceptable commands" is shown in Harkins at col. 2, lines 56-58. These portions describe configuration records that are compared by showing the differences between two builds of the program being debugged. Harkins neither discloses nor suggests the comparing element recited by the claims.

The rejection of claim 20 is therefore clearly erroneous, and claim 20 is not obvious in view of Desai and Harkins.

IV. <u>Claim Rejection: Claim 21</u>

Claim 21 was rejected as made obvious by Desai in view of Harkins and U.S. Pat. Pub. No. 2003/0154402 to Pandit. Claim 21 recites the limitations:

> observing commands that are accessing a database during a training phase, the commands comprising literal field data;...
> comparing commands that access the database during an operation phase with commands in the set of acceptable commands...

Thus, claim 21 explicitly recites a two-phase operation: a training phase when commands are observed; and an operation phase when commands are compared.

As explained above, the Examiner admits that Desai does not teach the "observing" and "comparing" elements and asserts that these elements are shown by Harkins. Harkins, however, neither teaches nor suggests observing or comparing. Moreover, Harkins does not teach or suggest the claimed two-phase operation where commands are observed during a training phase, and compared with commands that access the database during an operational phase. Pandit does not remedy the deficiencies of Desai and Harkins. Claim 21 is thus patentable over the cited references.

V. **Summary**

Based on the foregoing, Applicant respectfully submits that each of the pending rejections suffers from a clear deficiency in the prima facie case asserted in support of the rejection. Accordingly, Applicant requests that the rejections of claims 1 and 3-21 be withdrawn.

Respectfully submitted,
CAREY NACHENBERG AND FRANK BARAJAS

Dated: June 15, 2007

By: /Brian Hoffman/

Brian M. Hoffman, Reg. No. 39,713
Attorney for Applicant
Fenwick & West LLP
801 California Street
Mountain View, CA 94041
Tel.: (415) 875-2484
Fax: (415) 281-1350